Einige Teilbarkeitskriterien

Von LÁSZLÓ RÉDEI in Budapest

Prof. Béla Szőkefalvi-Nagy zum 60. Geburtstag gewidmet

§ 1

Für natürliche Zahlen $k(>1)$, a, n gilt das oft verwendete Teilbarkeitskriterium

$$k^a-1|k^n-1 \Leftrightarrow a|n. \tag{1}$$

Da n beiderseits offenbar nur mod a in Betracht kommt, genügt es (1) für den Fall $1 \leqq n \leqq a$ zu beweisen. In diesem Fall sind aber beide Seiten von (1) gleichbedeutend mit $a=n$. Folglich ist (1) allgemein richtig. Man sieht, daß in diesem Beweis auch von der Ordnungsrelation $<$ (oder, was auf dasselbe hinausläuft, von der Betragsbewertung des rationalen Zahlkörpers) Gebrauch gemacht wurde.

Für nichtkonstante Polynome $f(x)$ über einem Körper gilt ähnlich

$$f(x)^a-1|f(x)^n-1 \Leftrightarrow a|n. \tag{2}$$

Der Beweis ist dem vorigen ähnlich, mit dem geringen Unterschied, daß nach Reduktion auf den Fall $1 \leqq n \leqq a$ Gradvergleich (d.h. im wesentlichen Gradbewertung) hilft.

(1) und (2) lassen für beliebige Integritätsbereiche eine gemeinsame Verallgemeinerung zu (auch wenn keine Bewertung zur Verfügung steht).

Satz 1. *Für ein Element $\varkappa$ eines kommutativen Integritätsbereiches R mit Einselement ε und der Einheitengruppe E und für natürliche Zahlen a, n gilt das Teilbarkeitskriterium*

$$\varkappa^a-\varepsilon|\varkappa^n-\varepsilon \Leftrightarrow \varkappa^{(a,n)}=\varepsilon \wedge \left(\varkappa^{(a,n)} \neq \varepsilon \,\&\, \frac{\varkappa^a-\varepsilon}{\varkappa^{(a,n)}-\varepsilon} \in E\right), \tag{3}$$

wobei $\wedge$ und $\&$ als „oder" bzw. „und" zu lesen sind und (a, n) den größten gemeinsamen Teiler von a und n bezeichnet. (Der auftretende Quotient liegt in R, da sein Nenner ein Teiler des Zählers ist.)

(Der Leser sieht, daß (1) und (2) Spezialfälle von Satz 1 sind.)

Den Beweis von Satz 1 beginnen wir mit der Bemerkung, daß für jedes $\xi \in R$

$$\varkappa^a - \varepsilon | \xi \Leftrightarrow \varkappa^a - \varepsilon | \varkappa\xi \tag{4}$$

besteht. Hiervon ist der Teil $\Rightarrow$ trivialerweise richtig. Um den Teil $\Leftarrow$ zu beweisen, setzen wir die rechte Seite von (4) voraus. Dann gilt

$$\varkappa^a - \varepsilon | \varkappa^a \xi,$$

also gilt wegen $\varkappa^a \xi = (\varkappa^a - \varepsilon)\xi + \xi$ auch die linke Seite von (4). Somit ist (4) richtig. (Man sieht, daß im Beweis die Nullteilerfreiheit von R nicht ausgenutzt wurde.)

Nun ist der Teil $\Leftarrow$ von (3) trivialerweise richtig. Um den Teil $\Rightarrow$ zu beweisen, setzen wir die linke Seite von (3) voraus. Dann gelten

$$\varkappa^a - \varepsilon | \varkappa^{au} - \varepsilon, \quad \varkappa^a - \varepsilon | \varkappa^{nv} - \varepsilon$$

für alle natürlichen Zahlen u, v. Folglich gilt

$$\varkappa^a - \varepsilon | \varkappa^{au} - \varkappa^{nv}.$$

Für $au > nv$ entsteht hieraus nach (4)

$$\varkappa^a - \varepsilon | \varkappa^{au - nv} - \varepsilon.$$

Wählt man u und v so, daß

$$au - nv = (a, n)$$

gilt, so gewinnt man

$$\varkappa^a - \varepsilon | \varkappa^{(a,n)} - \varepsilon.$$

Da hieraus trivialerweise die rechte Seite von (3) folgt, ist Satz 1 bewiesen.

§ 2

Als ein „nächster" Schritt nach (1) *gilt für natürliche Zahlen* $k(>1)$, a, b, n *das Teilbarkeitskriterium*

$$(k^a - 1)(k^b - 1) | k^n - 1 \Leftrightarrow [a, b](k^{(a,b)} - 1) | n, \tag{5}$$

wobei $[a, b]$ *das kleinste gemeinsame Vielfache von* a *und* b *ist.*

Wir bemerken, daß (1) zum Beweis von (5) natürlich nicht ausreicht.

Ohne wesentlich größere Mühe beweisen wir den allgemeineren:

Satz 2. *Für ein Element* $\varkappa$ *eines Integritätsbereiches* R *mit dem Einselement* ε *und der Einheitengruppe* E *und für natürliche Zahlen* a, b, n *gilt das Teilbarkeitskriterium*

$$(\varkappa^a - \varepsilon)(\varkappa^b - \varepsilon) | \varkappa^n - \varepsilon \Leftrightarrow \varkappa^n = \varepsilon \wedge \left(\varkappa^n \neq \varepsilon \,\&\, \frac{\varkappa^a - \varepsilon}{\varkappa^{(a,n)} - \varepsilon}, \frac{\varkappa^b - \varepsilon}{\varkappa^{(b,n)} - \varepsilon} \in E \,\& \right. \tag{6}$$

$$\left. \& \, \varkappa^{(a,b,n)} - \varepsilon \left| \frac{(a, b, n) n}{(a, n)(b, n)} \varepsilon \right. \right).$$

(Der Leser sieht leicht, daß (5) in der Tat ein Spezialfall von Satz 2 ist.)

Im Fall $\varkappa^n = \varepsilon$ sind beide Seiten von (6) trivialerweise richtig. Deshalb setzen wir fortan

$$\varkappa^n \neq \varepsilon \tag{7}$$

voraus. Dann reduziert sich die Behauptung (6) auf

$$(\varkappa^a - \varepsilon)(\varkappa^b - \varepsilon) \mid \varkappa^n - \varepsilon \Leftrightarrow \frac{\varkappa^a - \varepsilon}{\varkappa^{(a,n)} - \varepsilon}, \frac{\varkappa^b - \varepsilon}{\varkappa^{(b,n)} - \varepsilon} \in E \,\&\, \varkappa^{(a,b,n)} - \varepsilon \mid \frac{(a,b,n)n}{(a,n)(b,n)} \varepsilon. \tag{8}$$

Wenn die linke Seite von (8) erfüllt ist, so sind $\varkappa^a - \varepsilon$ und $\varkappa^b - \varepsilon$ Teiler von $\varkappa^n - \varepsilon$, ferner folgt aus (7) offenbar

$$\varkappa^{(a,n)}, \varkappa^{(b,n)} \neq \varepsilon,$$

also muß nach Satz 1

$$\frac{\varkappa^a - \varepsilon}{\varkappa^{(a,n)} - \varepsilon}, \frac{\varkappa^b - \varepsilon}{\varkappa^{(b,n)} - \varepsilon} \in E \tag{9}$$

gelten. Deshalb setzen wir fortan auch (9) voraus. Dann reduziert sich die Behauptung (8) weiter auf

$$(\varkappa^a - \varepsilon)(\varkappa^b - \varepsilon) \mid \varkappa^n - \varepsilon \Leftrightarrow \varkappa^{(a,b,n)} - \varepsilon \mid \frac{(a,b,n)n}{(a,n)(b,n)} \varepsilon. \tag{10}$$

(Im folgenden Beweis von (10) wird von Satz 1 kein Gebrauch mehr gemacht.)

Wir schicken den Beweis für den Fall

$$(a,b,n) = 1 \tag{11}$$

voraus. Gleich bemerken wir, daß aus (11)

$$(a,n)(b,n) \mid n, \quad ((a,n),(b,n)) = 1 \tag{12}$$

folgen.

Wir benötigen eine kleine Vorbereitung. Hierzu nehmen wir zwei teilerfremde natürliche Zahlen r, s und setzen

$$f(x) = \frac{(x^{rs} - \varepsilon)(x - \varepsilon)}{(x^r - \varepsilon)(x^s - \varepsilon)}, \tag{13}$$

wobei Zähler und Nenner als Elemente des Polynomringes $R[x]$ zu deuten sind. Da aber $x - \varepsilon$ im Ideal $(x^r - \varepsilon, x^s - \varepsilon)$ liegt, gilt wegen (13)

$$f(x) \in R[x]$$

offenbar. Da ferner der Ersetzungswert eines Polynoms von der Form

$$\frac{x^i - \varepsilon}{x - \varepsilon} \in R[x] \qquad (i = 1, 2, \ldots)$$

für $x=\varepsilon$ gleich $i\varepsilon$ ist, folgt aus (13) $f(\varepsilon)=\varepsilon$. Andererseits ist $f(\varkappa)\equiv f(\varepsilon) \pmod{\varkappa-\varepsilon}$, also gilt

$$f(\varkappa) \equiv \varepsilon \pmod{\varkappa-\varepsilon}. \tag{14}$$

Nun ist die linke Seite von (10) wegen (9) gleichbedeutend mit

$$(\varkappa^{(a,n)}-\varepsilon)(\varkappa^{(b,n)}-\varepsilon) \mid \varkappa^n-\varepsilon.$$

Wegen (7) und (12) formt sich diese Teilbarkeit identisch in

$$(\varkappa^{(a,n)}-\varepsilon)(\varkappa^{(b,n)}-\varepsilon)(\varkappa-\varepsilon) \mid \frac{\varkappa^n-\varepsilon}{\varkappa^{(a,n)(b,n)}-\varepsilon}(\varkappa^{(a,n)(b,n)}-\varepsilon)(\varkappa-\varepsilon)$$

um. Verwendet man (13) mit $r=(a,n)$, $s=(b,n)$ (die hierzu nötige Bedingung $(r,s)=1$ ist nach (12_2) erfüllt), so entsteht (nach Kürzung) die weitere äquivalente Umformung

$$\varkappa-\varepsilon \left| \frac{\varkappa^n-\varepsilon}{\varkappa^{(a,n)(b,n)}-\varepsilon} f(\varkappa). \right.$$

Da sich der zweite Faktor der rechten Seite wegen (14) streichen läßt und der erste Faktor kongruent

$$\frac{n}{(a,n)(b,n)}\varepsilon$$

mod $\varkappa-\varepsilon$ ist, ist (10) für den Fall (11) bewiesen.

Der allgemeine Fall läßt sich leicht auf den vorigen zurückführen. Zu diesem Zweck setzen wir

$$d=(a,b,n), \quad \lambda=\varkappa^d.$$

Dann ist (10) gleichbedeutend mit

$$(\lambda^{\frac{a}{d}}-\varepsilon)(\lambda^{\frac{b}{d}}-\varepsilon) \mid \lambda^{\frac{n}{d}}-\varepsilon \Leftrightarrow \lambda-\varepsilon \mid \frac{\frac{n}{d}}{\left(\frac{a}{d},\frac{n}{d}\right)\left(\frac{b}{d},\frac{n}{d}\right)}\varepsilon,$$

ist also nach vorigem Resultat richtig. Somit ist Satz 2 bewiesen.

(Eingegangen am 11. März 1972)